


Mayer Hoffman McCann P.C.

An Independent CPA Firm

Conrad Government Services Division

2301 Dupont Drive, Suite 200

Irvine, California 92612

949-474-2020 ph

949-263-5520 fx

www.mhm-pc.com

Finance and Administration Committee
Orange County Transportation Authority
Orange, California

In planning and performing our audit of the financial statements of the Orange County Transportation Authority (OCTA) as of and for the year ended June 30, 2008, in accordance with auditing standards generally accepted in the United States of America, we considered OCTA's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of OCTA's internal control. Accordingly, we do not express an opinion on the effectiveness of OCTA's internal control.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects OCTA's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of OCTA's financial statements that is more than inconsequential will not be prevented or detected by OCTA's internal control. Matters conforming to this definition are identified below.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by OCTA's internal control. Our consideration of internal control was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

(1) Need to Strengthen Controls of Third-Party Contractor

OCTA utilizes a third-party contractor (contractor) to manage and oversee the State Route 91 Toll Road (Toll Road) revenue cycle. The information systems of the contractor are significant to the financial information of OCTA. As such, we reviewed the information systems of the contractor to ensure that controls were designed and implemented to mitigate risk of loss of OCTA assets. During this review, we noted the following issues:



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(1) Need to Strengthen Controls of Third-Party Contractor (Continued)

- Tape backups of all files, including master files, transactions files, application programs, systems software, and database software that support Toll Road operations, are currently stored on-site at the third-party contractor's office. The contractor has elected to maintain tape backups onsite based on current business concerns. Industry best practice recommends using a backup storage site that is geographically removed from the primary site. In the event of a catastrophic event at the main office location, information would be lost without a means for recovery.
- The system used to track customer account and vehicle information has password controls that are limited to a minimum of 6 characters, with no complexity requirements or user lockout after a certain number of unsuccessful log-in attempts. Effective password complexity controls were not considered during system implementation. Controls recommended by industry best practice include:
 - a. Alphanumeric passwords;
 - b. Required password change interval; and
 - c. Locking user accounts after a maximum number of incorrect password attempts.

Without effective password controls, an unauthorized user could employ various forms of password hacking tools to access the system.

- The process to remove terminated employees from systems is manual and not synchronized to a master employee database. In addition, of the 5 terminated users sampled, one user was not removed from the active directory network in a timely manner. Industry best practice suggests removing user access to systems immediately following termination. Untimely removal of users' access after termination provides employees an opportunity to sabotage or otherwise impair entity operations or assets.

The aggregate effect of these weaknesses in information systems controls increases the likelihood of theft, loss or misuse of OCTA assets.

Recommendation

We recommend that the third-party contractor be required to establish procedures to strengthen internal controls in the information systems associated with the OCTA contract.



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(1) Need to Strengthen Controls of Third-Party Contractor (Continued)

Management's Responses

Staff agrees with the auditors' recommendation regarding backup tapes. The Authority's operator, Cofiroute USA (Cofiroute), had been maintaining backup tapes at the Anaheim Office for research purposes related to ongoing litigation against the Authority. However, all backup tapes have now been stored at a secure, offsite location with Iron Mountain.

Staff agrees with the auditors' recommendation regarding password controls. For Cofiroute employees to access the system used to track customer account and vehicle information, TollPro, requires the user to first login to the domain. Cofiroute controls access to the domain. The password complexity for the domain is as follows:

- a. The password cannot contain all or part of the user's account name
- b. The password must be at least seven characters in length
- c. The password must contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphanumeric characters (&, \$, #, %, etc.)
- d. The user is automatically logged off if the domain is not accessed for 10 minutes
- e. After five invalid logon attempts, the account will be locked out.

Once the domain is accessed, the user must then enter a TollPro password. The TollPro system currently does not have the password complexity requirements identified above with the Cofiroute login procedures. The system developer of TollPro, Northern Lakes Data Corporation, will be modifying the password complexity to match industry best practices.

Staff agrees with the auditors' recommendation of removing user access to systems immediately following termination. Cofiroute's practice is to remove employees by the end of the following business day for terminated employees. In the example cited in the finding, an employee was terminated on the Friday prior to the Thanksgiving week of 2007. The Human Resources employee responsible for removing terminated employees was on vacation during that week. Therefore, the terminated employee was not removed from the system until the following Monday, ten days after the day of termination. Cofiroute will implement a policy to ensure all terminated employees are removed by the close of the following business day.



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(1) Need to Strengthen Controls of Third-Party Contractor (Continued)

Cofiroute is an independent contractor responsible for managing 91 Express Lanes operations for the Authority. The TollPro system that is used to track customer account and vehicle information is a proprietary system developed and maintained by Northern Lakes Data Corporation and is not connected to the Cofiroute management system or Human Resources records. Cofiroute maintains Human Resources data at its corporate office in Irvine. TollPro and Cofiroute systems are completely independent and not technically compatible. Cofiroute does not permit access of the TollPro system from computers other than those owned by the 91 Express Lanes. Cofiroute employees can only access TollPro through a Cofiroute controlled computer and domain.

(2) Internal Controls over the Combined Transportation Funding Program

During our search for unrecorded liabilities, we noted two cash disbursements related to Combined Transportation Funding Program (CTFP) Agreements between OCTA and the City of Anaheim (City) that should have been accrued as of June 30, 2008.

According to Project Delivery Department personnel, the cash disbursements were not issued to the City during fiscal year 2007-08 as the required documentation was furnished to OCTA subsequent to year-end. However, all of the supporting documentation submitted to OCTA was dated January 2008. As a result, the Accounting Department posted an adjustment for \$6,375,355 to accrue this liability as of June 30, 2008.

Recommendation

We recommend that the Project Delivery Department ensure proper documentation is maintained regarding any withholding or delay of payments resulting from lack of documentation provided by the entity awarded CTFP funds.

Management's Response

Staff is currently developing an electronic tracking system that will facilitate the audit recommendation. This effort was in process prior to the audit report. Once completed, the system will provide an electronic log of invoice issues, missing documentation, correspondence with the cities, and track the dates missing documentation is both requested and received.



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(3) Communication of Financial Information to the Appropriate Department

During our review of fund balances, we noted one instance where revenues related to cooperative agreements entered into by OCTA were improperly accrued in prior years and had to be adjusted in the current year. The amount of the prior year adjustment was \$4,114,302. The primary cause of this was lack of communication of changes in cooperative agreements by Project Managers to the Financial Planning and Analysis Department (FP&A) or the Accounting Department. The cooperative agreement changes and amendments appear to involve OCTA's Planning Department, which does not always communicate amendments to agreements to FP&A and Accounting.

Recommendation

We recommend OCTA establish procedures or protocols to ensure that all information of a financial nature is communicated to the FP&A Department or Accounting Department, as appropriate.

Management's Response

This was a unique situation that is unlikely to be repeated. The original cooperative agreement with Caltrans referred to the "latest revision" of a standard funding agreement as the appropriate documentation for the subject funding amount. This funding agreement was revised a couple of times, but a change to the document did not require the original cooperative agreement to be amended. If an amendment were to be made to the agreement, it would have been transmitted to FP&A by the Contracts Administration and Material Management (CAMP) Department. This was an unusual structure for a cooperative agreement that is unlikely to be repeated. The normal processing and transmittal of agreements and amendments by CAMP should provide the required financial information needed by FP&A.

(4) Need to Establish a Policy on Misconduct

OCTA does not currently have a written policy on misconduct. An effective method of communicating and reinforcing an antifraud culture within an organization is through the development of a policy on misconduct. A misconduct policy communicates to all employees the organizational position and policy on matters such as the following:

- Risks that the organization faces from fraud, abuse and other forms of misconduct;
- Effect of the Code of Conduct;
- Definitions of misconduct, including fraud and abuse;



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(4) Need to Establish a Policy on Misconduct (Continued)

- Employee's responsibility to report suspected misconduct (including an established reporting mechanism, such as a member of the Board of Directors, a consultant or advisor, hotline service, etc.);
- Organizational responsibility to investigate; and
- Disciplinary action for violations

Best practice suggests that a misconduct policy and its annual reaffirmation by employees will greatly strengthen internal controls to prevent the occurrence of fraud and abuse. The policy should be acknowledged and signed by each employee upon hire and on an annual basis as evidence of their affirmation that they understand the policy and have complied with its provisions. This condition was also reported for the year ended June 30, 2007 in our communication dated October 31, 2007.

Recommendation

OCTA should develop and implement a policy on misconduct. Once developed, the policy should be acknowledged and signed by each employee on an annual basis as evidence of their affirmation that they understand the policy and have complied with its provisions.

Management's Response

Management will develop and implement a policy on misconduct; each new hire will be asked to acknowledge and sign the policy upon starting work at OCTA.

(5) Need to Adhere to Buy America Requirements

OCTA's rolling stock procurement documentation did not meet the Post-Delivery Procurement Audit requirements per the Federal Transit Administration (FTA) Buy America Handbook. According to Section 3 of the Buy America Handbook, purchases of 10 buses or more must have the resident inspector complete a final manufacturing report, which should include any information that supports or refutes claims made by the manufacturer concerning its capabilities or the bus specifications. For buses manufactured in multiple stages (such as body-on-chassis buses), the resident inspector is required to visit the final-stage manufacturer's final assembly location only. Once completed, the Post-Delivery Purchaser's Requirement Certification is made and filed.



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(5) Need to Adhere to Buy America Requirements, (Continued)

OCTA provided the sign-off of contract completion as proof of the post-delivery review for the rolling stock purchases reviewed. However, the documentation does not provide sufficient evidence that OCTA verified that the Buy America information had not materially changed from the pre-award stage to the completed manufacturing stage. This condition was also reported for the year ended June 30, 2007 in our communication dated October 31, 2007.

Recommendation

We recommend that OCTA adhere to the Buy America requirements and ensure that all documentation is contained in the procurement files to support OCTA's compliance.

Management Response

The OCTA Transit Division Maintenance Department inspectors will follow the Buy America guideline as done last year. OCTA will insure that contract administration has the necessary paperwork on file for the closing of contracts for the post filings.

In addition, we observed the following other matters, which were not deemed to be significant deficiencies or material weaknesses, and offer these comments and suggestions:

(6) Segregation of Duties in the Payroll Process

Two individuals who have the ability to prepare and transmit the positive pay file to the bank for payroll are System Administrators in the Information Technology Department. These individuals were identified in the Lawson payroll system as "ADMIN" security class and had access to all Lawson forms and programs. As a result, there is an increased risk that these individuals could make unauthorized pay rate changes to the system without it being detected by management.

Recommendation

No recommendation is warranted. In May 2008, OCTA upgraded its Lawson application. As a result, the security plan was changed from the initial implementation package and the access for the two individuals was limited to specific functions based on job duties.



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(7) Setting up New Vendors in Accounts Payable Module

The Accounts Payable Supervisor and two Accounts Payable Technicians have access to create and edit vendors in the Integrated Financial and Administrative Solution (IFAS) accounts payable module. To mitigate the risk of unauthorized payments being issued, individuals responsible for processing cash disbursements should not be able to create and edit vendor information.

Recommendation

No recommendation is warranted. In June 2008, the Accounting Department reassigned the responsibility of creating and editing vendor information to an individual who is not responsible for processing cash disbursements and restricted the access for the Accounts Payable Technicians so they are not able to create or edit vendors in the system. In addition, the Accounts Payable Supervisor currently reviews a report generated by IFAS that identifies all new vendors created during each accounts payable check run.

(8) Need to Establish a Formal Change Management Process

There was no documented change management process in place for most of the year ended June 30, 2008. Change management is the process of documenting changes to computer applications, from the time a request for a change is made through the time in which the change is placed into the production environment. The following specific conditions were noted during our review of the informal change management process:

- All changes are generally initiated in the Information Systems (IS) Help Desk System through the creation of a ticket, but are not tracked through completion. Eventually all tickets are closed. Additionally, the Help Desk System is not always utilized for all changes.
- Significant changes are handled within a project and assigned to an OCTA project manager. The OCTA project manager may or may not create a project plan or other tracking mechanism for IS changes.
- Changes to various systems are maintained by the various system administrators, but the change documentation is not standardized or centralized in one location.

A documented change management process will mitigate the risk of unauthorized changes to hardware, applications, and systems.



Finance and Administration Committee
Orange County Transportation Authority
Orange, California

(8) **Need to Establish a Formal Change Management Process (Continued)**

Recommendation

OCTA developed and implemented a formal change management process. The process documents the system development cycle of changes to hardware, applications, and systems effective June 2008. As such, this condition has been resolved.

OCTA's written responses to the significant deficiencies identified in our audit are described above. We did not audit OCTA's responses, and accordingly, we express no opinion on them.

This communication is intended solely for the information and use of management, the Board of Directors, the Finance and Administration Committee, others within the organization, and federal and pass-through awarding agencies and is not intended to be and should not be used by anyone other than these specified parties.

Margaret Holburn McCann PC

Irvine, California
October 24, 2008